CLAIM AMENDMENTS

Please amend the claims as follows:

1. (Currently Amended) A method of pre-processing content in a video on demand (VOD) system, wherein the content is identified by a first set of packet identifiers (PIDs), the method comprising:

carrying out the following process at a VOD service provider site:

receiving content, the content having marked packets designating packets that are to be encrypted by a first encryption system, the packets that are to be encrypted being marked by a set encryption flag for all packets designated to be encrypted;

selecting packets in the content according to a selective encryption selection criterion to produce selected packets;

at a packet duplicator, duplicating the selected packets to produce duplicate copies of the original packets;

identifying the duplicate copies using a second set of PIDs;

inserting the duplicate copies of the original packets identified by the second set of PIDs into the content;

clearing all encryption flags in the content except for the selected packets having the first set of PIDs, thereby producing content having identifiable duplicate selected packets suitable for selective encryption;

encrypting the content having the identifiable duplicate selected packets using the first encryption system;

storing the encrypted content having the identifiable duplicate selected packets and the duplicate copies at a VOD server for a period of time during which the VOD server awaits receipt of a request for the content from a subscriber device; and

receiving the request ~~a request~~ for the stored content from a subscriber device that uses a second encryption system, and in response to the request at the VOD server:

retrieving the content from storage;

stripping out the encrypted content having the identifiable duplicate selected packets; and

encrypting the duplicate copies using the second encryption system.

2. (Original) The method according to claim 1, wherein the encryption flag is encoded using transport_scrambling_control data bits.

3. (Previously Presented) The method according to claim 1, further comprising:

identifying packets of content used in trick play modes; and

creating at least one trick mode content file and creating forward and reverse trick mode index tables.

4. (Original) The method according to claim 3, further comprising modifying the forward and reverse trick mode index tables to account for insertion of the duplicate copies.

5. (Original) The method according to claim 3, wherein the packets of content used in trick play modes comprise intra-coded frames.

6. (Previously Presented) The method according to claim 3, further comprising storing the at least one trick mode file and the forward and reverse trick mode index tables on the VOD server.

7. (Original) The method according to claim 1, further comprising generating a program association table (PAT) and a program map table (PMT) identifying the second set of PIDs.

8. (Previously Presented) The method according to claim 7, further comprising, storing the PAT, the PMT, and the content on the VOD server.

9. (Original) The method according to claim 3, further comprising generating a program association table (PAT) and a program map table (PMT) identifying the second set of PIDs.

10. (Previously Presented) The method according to claim 9, further comprising storing the at least one trick mode file and the forward and reverse trick mode index tables, the PAT, the PMT, and the content on the VOD server.

11. (Cancelled)

12. (Previously Presented) The method according to claim 1, wherein the encryption under the first encryption system is carried out in an off line encryption system.

13. (Previously Presented) The method according to claim 1, further comprising storing the forward and reverse trick mode files, the forward and reverse trick mode index tables, the PAT, the PMT, and the content on the VOD server.

14. – 17. (Cancelled)

18. (Original) The method according to claim 1, further comprising adjusting a program clock reference (PCR) in packets containing adaptation fields to account for insertion of the duplicate copies.

19. (Original) The method according to claim 1, further comprising deleting null packets to compensate for insertion of the duplicate copies.

20. (Original) The method according to claim 1, wherein the selecting, duplicating, identifying, inserting and clearing functions are carried out in an offline selective encryption processor (OSEP).

21. (Previously Presented) The method according to claim 9, wherein the packets are marked in the VOD server.

22. (Currently Amended) A method of processing content in a video on demand (VOD) system, wherein the content is identified by a first set of packet identifiers (PIDs), the method comprising:

carrying out the following process at a VOD service provider site:

identifying packets of content used in trick play modes;

creating at least one trick mode file and forward and reverse trick mode index tables;

marking packets in the content to be encrypted by a first encryption system by setting an encryption flag for all packets designated to be encrypted;

selecting packets in the content according to a selective encryption selection criterion to produce selected packets;

at a packet duplicator, duplicating the selected packets to produce duplicate copies of the selected original packets;

identifying the duplicate copies using a second set of PIDs;

generating a program association table (PAT) and a program map table (PMT) identifying the second set of PIDs;

inserting the duplicate copies identified by the second set of PIDs into the content;

clearing all encryption flags in the content except for the selected packets having the first set of PIDs, thereby producing content having identifiable duplicate selected packets suitable for selective encryption;

encrypting the content having the identifiable duplicate selected packets using the first encryption system;

storing the at least one trick mode file and the forward and reverse trick mode index tables, the PAT, the PMT, and the encrypted content having the identifiable duplicate selected packets and the duplicate copies at a VOD server for a period of time during which the VOD server awaits receipt of a request for the content from a subscriber device;

receiving the request ~~a request~~ for the stored content from a subscriber device that uses a second encryption system;

retrieving the content from storage;

stripping out the encrypted content having the identifiable duplicate selected packets in response to the request at the VOD server; and

encrypting the duplicate copies using the second encryption system in response to the request.

23. (Original) The method according to claim 22, wherein the encryption flag is encoded using transport_scrambling_control data bits.

24. (Cancelled)

25. (Previously Presented) The method according to claim 22, wherein the encryption under the first encryption system is carried out in an off line encryption system.

26. (Cancelled)

27. (Original) The method according to claim 22, further comprising modifying the forward and reverse trick mode index tables, deleting null packets and adjusting a program clock reference (PCR) in packets containing adaptation fields to account for insertion of the duplicate copies prior to the storing.

28. (Previously Presented) The method according to claim 22, further comprising retrieving the encrypted content having the identifiable duplicate selected packets and the duplicate copies from the VOD server.

29. (Currently Amended) A selective encryption system for use in a video on demand (VOD) system, comprising:

the system residing at a VOD service provider site:

a selective encryption processor that receives content, the content containing packets that are marked for encryption by a first encryption system, the packets being marked by having a set encryption flag for all packets marked for encryption;

the selective encryption processor processing the content for storage on a VOD server, wherein the content is identified by a first set of packet identifiers (PIDs), the selective encryption processor comprising:

a packet selector that selects packets in the content according to a selective encryption selection criterion to produce selected packets;

a packet duplicator that duplicates the selected packets to produce duplicate copies of the selected packets and identifies these duplicate copies using a second set of PIDs when the duplicate copies are inserted into the content; and

an encryption flag manager that clears all encryption flags in the content except for the selected packets having the first set of PIDs; and

an off line encryption system that encrypts packets having a set encryption flag under the first encryption system;

a memory that stores the content for a period of time during which the VOD server awaits receipt of a request for the content from a subscriber device

an add/drop re-multiplexer at the service provider site that deletes the encrypted packets in response to receiving the request ~~a request~~ for the content from a target subscriber receiver that uses a second encryption system; and

a session based encrypter that encrypts the duplicate copies using the second encryption system in response to the request for the content from the target receiver that uses the second encryption system.

30. (Previously Presented) A selective encryption system for use in the video on demand system according to claim 29, wherein the encryption flag is encoded using transport_scrambling_control data bits.

31. (Previously Presented) A selective encryption system for use in the video on demand system according to claim 29, further comprising a trick play file processor that identifies packets of content used in trick play modes and creates at least one trick mode file and forward and reverse trick mode index tables.

32. (Previously Presented) A selective encryption system for use in the video on demand system according to claim 31, further comprising a timing corrector that modifies the forward and reverse trick mode index tables to account for insertion of the duplicate copies.

33. (Previously Presented) A selective encryption system for use in the video on demand according to claim 32, wherein the timing corrector further deletes null packets and adjusts a program clock reference (PCR) in packets containing adaptation fields to account for insertion of the duplicate copies.

34. (Previously Presented) A selective encryption system for use in the video on demand system according to claim 29, further comprising a PMT/PAT generator that generates a program association table (PAT) and a program map table (PMT) identifying the second set of PIDs.

35. – 36. (Cancelled)

37. (Previously Presented) A selective encryption system for use in the video on demand system according to claim 29, where the add/drop re-multiplexer is further configured to delete either the selected packets or the duplicate copies depending upon a target receiver's decryption capability.

38. (Previously Presented) A selective encryption system for use in the video on demand system according to claim 29, further comprising:

a trick play file processor that identifies packets of content used in trick play modes and creates at least one trick mode file and forward and reverse trick mode index tables;

a PMT/PAT generator that generates a program association table (PAT) and a program map table (PMT) identifying the second set of PIDs; and

a VOD server that stores the at least one trick mode file, the forward and reverse trick mode index tables, the PAT, the PMT, and the content.

39. (Previously Presented) The method according to claim 5, further comprising smoothing trick mode transition recovery by skipping certain packets following intra-coded frames using dynamic substitution.

40. (Previously Presented) The method according to claim 22, further comprising smoothing trick mode transition recovery by skipping certain packets following intra-coded frames using dynamic substitution.

41. (Previously Presented) A selective encryption system for use in the video on demand system according to claim 31, where the trick play file processor smoothes trick mode transition recovery by skipping certain packets following intra-coded frames using dynamic substitution.